AutoBlocker: A Netflow based traffic anomaly detector and blocking engine.

Review of Status and Project proposal

by Andrey Bobyshev, CD/LCS/NVS/NS

August 8, 2010

Table of Contents

Purpose of this document

The purpose of this document is to review status of AutoBlocker tool used at Fermilab as a protective measure at the network perimeter, identify its major issues and areas that need an improvement. This document is aimed to either initiate a project to address current issues of AutoBlocker or to replace it by some other tool.

Introduction

AutoBlocker is a tool developed at Fermilab by Networking for Computer Security and Networking needs on detection of traffic anomaly and prevention or mitigation of negative impact on the mission and image of the Laboratory by blocking sources of traffic that is considered as excessive or malicious and/or not related to the mission of the Laboratory.

This tool has been developed in 2002 as the result of collaborative efforts of Networking and Computer Security groups and deployed on October 23 of 2002. It is almost eight years as this tool is in production 24x7x365. There were only a few minor changes since its initial deployment. At same time the original network environment has changed significantly.

In last 5-6 years there were several attempts to find a replacement for AutoBlocker. I am not aware of any definitive plans or any activity started. As person involved in design, development and operation of this tool I think, it is about time to review status of AutoBlocker and make a decision either to initiate a project to improve it or to replace it by some other tool.

Status of AutoBlocker

The AutoBlocker is a tool that combines a traffic anomaly detector and a blocking engine. AutoBlocker's detector is based on passive analysis of netflow data gathered from border routers. a
The main AutoBlocker's features are:

- analyzing netflow from multiple exporters, currently it is configured to analyze data exported from border routers
- support of multiple detectors, not necessarily based on netflow analysis. It has currently two detectors, an embedded netflow-based one and an external one to detect slow scanning
- multiple levels of threats (red, yellow, green..)
- multiple actions such as block/unblock, watch, notice associated with each threat level
- multiple notifications, e-mail, XML-message to NIMI (stopped working in ~2006/7 after changes on the NIMI side)
- XML(SOAP) interface
- automatic deployment of blocking/unblocking actions to multiple devices in parallel

- Web-interface to see detailed information about AutoBlocker's events. It also allows to submit administrative block/unblock requests
- adaptive algorithms to expire active blocks depending on utilized resources

Major issues

1. The limited size of ACL to be applied to a router. In fact, this limitation comes from router's side. AutoBlocker replaces ACLs very frequently, almost every minute. If ACL is too big, it becomes CPU intensive job for router to update it. In such a case CPU load can reach 100% and affects router's capability to forward packets. In order to avoid that AutoBlocker causes 100% CPU load of the advanced routers such as Catalyst 6509 with Supervisor 720B/BXL, the limit of ~1000 entries needs to be configured on AutoBlocker's side. In order to maintain such a limit AutoBlocker has to expire oldest entries earlier than Computer Security would like to guarantee them. For example, CST wants to keep detected offsite intruders blocked for several days, while ACL limits force to expire these blocks in several hours if they stopped malicious activity.

> An issue of frequent ACL updates has been addressed in the LambdaStation project that deals with a similar task to modify router's configuration dynamically.

2. False alerts on detection of traffic anomalies. Autoblocker uses an approach of calculating multiple metrics for inspected traffic and evaluating these metrics against pre-defined thresholds. The initial metrics and thresholds developed eight years ago were good for traffic pattern typical at that time. Nowadays applications become more and more distributed and aggressive in terms of probing various networking resources and other servers. It will need a special research of typical traffic pattern and investigation of various heuristic algorithms to be added into data analysis of AutoBlocker's detectors.

> The Networking and Computer Security groups at Fermilab have a long history of using netflow for various analysis of application's performance, searching of vulnerabilities and investigation of computer security incidents. That experience was not yet available when AutoBlocker has been deployed. The capabilities of routers on exporting flow data have also changed in last eight years.

3. Current implementation of AutoBlocker's configuration limits capability to view/modify it by authorized personal other than one who operates it and has direct access to its configuration

4. AutoBlocker has the XML/SOAP interface to obtain its status information and submit selected operator's commands but it did not reach mature and stable level. That is why there was only limited use of its capabilities, mainly for monitoring of deployed blocks.

> On-going ESCPS project and completed Lambda Station project are(were) dealing with the similar issues of creating Web Services/XML based interfaces for multi-platform environment for controlling of network infrastructure. An experiences of these projects can be utilized to address that Autoblocker's issue.

The complete list of issues that might need an improvement is outside of the scope of this document. It should be a part of design phase of new project on upgrade AutoBlocker if decided. Four listed above should be sufficient to justify the need for AutoBlocker's needs upgrade or a replacement.

Project proposal

The purpose of this document is to define need for a project that could address current AutoBlocker's issues within a reasonable short period time of 6 - 8 months. The project itself, if decided, will need an additional analysis and design work. Here are the major areas that will need efforts:

- Improve detection module(s) of AutoBlocker. Experience gained by other related projects or activities completed in recent years and on-going ones could be utilized as well.
- Develop a single general service for configuring of network resources. There are several applications at Fermilab that are tasked to modify various parts of the network. It might cause conflicts if multiple applications will configure same network resources without synchronization. The ongoing DOE-funded ESCPS project is being designed and developed with such approach in mind when it needs to change configuration of network on-demand of applications
- Support of other router's platforms that have been deployed at Fermilab, such as Nexus 7000 (NETCONF protocol)

Estimation of resources needed

An estimation of resources needed for the project to address most critical issues of AutoBlocker with the goal to complete it within 6-8 months

Man-power/expertise resources:

- Network analyst/architect/engineer, 02 FTE
- A network/computer science researcher, netflow analysis, investigation/developing of heuristics algorithms of data analysis, 0.4FTE
- Software engineer 0.6

Computing/networking resources:

- A testbed with 2-3 routers running IOS (6509), NX-OS (Nexus 7000/5000).
- Computing resources: 2- 3 low/middle class servers

A timeline

1. Review of current AutoBlocker algorithms, design - 1- 2 months
2. Design/prototyping/testbed setup, 2-4 months
3. Development, 3 - 4 months